Outcomes High-Level Meeting Cyber Security

Amsterdam, 12 and 13 May 2016

1. Introduction and practical overview

On 12 and 13 May 2016 the High-Level Meeting Cyber Security, which was an important part of the Netherlands EU presidency, took place in Amsterdam. At the meeting, the public and the private sector came together to discuss current trends in the digital domain and which opportunities and risks those contain for the future of cybersecurity. The evening before the High Level Meeting twenty experts in the field of cyber security from the public, private and academic sectors had a fruitful discussion, organised by the Dutch Cyber Security Council, on Internet of Things and harmonization of duties of care in Europe.[1]

2. Key findings

The continued digitalisation of society and the economy, sometimes named the fourth industrial revolution, presents new and quickly growing challenges and risks, ranging from cybercrime, to (economic) espionage, to privacy issues, to (potential) attacks on critical infrastructure. A number of participants stated that the we ought to be concerned not if but when such attacks will indeed take place. When such (large-scale) attacks or incidents do to take place, strong cross-border cooperation and cooperation between the public and private sector is necessary. This development also affects non-traditional cyber sectors, of which road transport and aviation were discussed at the meeting. It was generally agreed that urgent action in addition to existing/ running programmes is necessary.

While there are no quick fixes, the completion of the NIS Directive together with other recent initiatives within the Digital Single Market form the foundation for strong, effective and consistent EU-wide cross-border cooperation that can respond to the challenges above. A swift implementation of the NIS Directive was therefore strongly recommended.

An advice that was often given during the meeting was to focus not only on the governmental groups created through the NIS Directive, but also to find ways to engage experts from the private sector, academia and the internet community, both at the national and European level. Such partnerships can maximise the exchange of information and will position all involved to seize the opportunities that digitalisation offers while ensuring the safety of its citizens. Leadership by the EU and Member States, for example in the field of standards, was therefore encouraged.[2]

3. Recommendations

A swift implementation of the NIS Directive is of critical importance to set the first steps towards responding to the identified developments and challenges. In addition to the NIS Directive, however, more steps and actions are needed to create cybersecurity policies and approaches that will

[1] The result he conclusions and recommendations of this meeting and the papers written by the participants will be presented to the director general DG Connect.

[2] An infographic presenting the key findings visually can be found here.

prepare us for the future after the NIS Directive's implementation, through inter alia:

Engaging the private sector

The complex, rapidly developing and diffuse ICT domain makes it impossible for governments, with an inherently (geographically) limited reach, to address these challenges alone. Therefore the exchange of information, which was believed to be critical, at the at the European and national level is necessary. This should include both the private sector and the broader internet community.

When it comes to engaging the private sector a particular focus in the discussions lay on the added value of **Public-Private Partnerships** (PPP) in a European perspective. It was concluded that that European cooperation in this regards is essential. The logical next step is an evolution of national PPP communities towards European PPP communities.

Such an evolution was seen as the logical next step to address the current fragmentation and towards more cross-border public-private cooperation, through the creation of Information Sharing and Analysis Centres (ISACs) and otherwise. Such an approach can also contribute to a harmonised implementation of the NIS Directive in the different Member States, which will contribute to a level-playing field within the EU. This evolution can address the current fragmentation and contribute towards more cross-border public-private cooperation, for instance through the creation of European Information Sharing and Analysis Centres (ISACs). Such an approach can also contribute to a harmonized implementation of the NIS Directive in the different Member States, which will contribute to a level-playing field within the EU.

At the strategic level, foresights on cyber developments drafted by fora consisting of high-level officials from the public sector, the private sector and academia are valuable to provide a solid basis for future cyber policy. While such councils, fora and initiatives exist in a number of Member States, it was recommended that such fora are formed and/or strengthened at the EU level.

Due to the completion of the NIS directive, most attention is expected to be given to cooperation with the critical infrastructure operators. Identified future developments such as the rise of the Internet of Things, however, compel a much broader collaborative effort that involves not only critical infrastructure operators, but all stakeholders, including device manufacturers, software producers, policy makers, solution integrators and security researchers.

To promote this cooperation the following actions were recommended:

- Increase institutionalised cooperation with private stakeholders.
- Examine whether positive incentives can be provided to operators of critical infrastructure to invest in security measures.
- Develop and conduct a maturity assessment of Member States' critical infrastructure protection readiness.

A challenge will be to balance the need for mandatory incident reporting versus the benefits of voluntary cooperation and information sharing based on trust building.

Innovative, non-legislative approaches and best practices to engage the internet community were discussed. One approach that was highlighted in particular was the so-called ***Coordinated Vulnerability Disclosure* approach**. This approach calls upon organisations to be receptive to reports from ‘the internet community’ on possible security risks and vulnerabilities in their systems, infrastructure and/or products and to refrain from taking legal action against the reporter(s) under certain conditions. This helps organisations to repair vulnerabilities in their systems and make them as safe as possible. During the meeting over twenty-eight companies and organisations signed a Coordinated Vulnerability Disclosure manifesto in which they pledge to implement a Coordinated Vulnerability Disclosure policy and promote the contents of the manifesto to their peers.[3]

Besides threats to respond to, the digitalisation of the economy and society also present economic opportunities for the cybersecurity industry, which is one of fastest growing markets globally in the ICT sector. A strong cybersecurity industry can also support a flourishing European digital single market, and help European companies compete and grab the opportunities deriving from such a booming market. The EU’s contractual Public-Private Partnership (cPPP) was identified as an important vehicle to contribute to this. To maximise its impact, it was recommended that there is strong participation from both industry and the Member States.

Strengthening resilience

Besides engaging the private sector, governments can and should focus on measures and approaches to strengthen resilience as well. This can happen in the fields of education, awareness raising, standardisation and certification. European action in these areas was identified as necessary.

In the field of **education** the main challenge facing Europe is a significant shortage in the number of cybersecurity experts. There are some projections that indicate a shortfall of 800.000 of such professionals by 2020.

To reduce this expected gap the following actions were recommended:

- An integrated approach targeting all levels of education, starting at elementary school. This approach should include both basic **cyber awareness and digital literacy,** as well as more specialised skills such as programming, coding and computational thinking. Including awareness elements in popular activities can help reach a large audience.
- Educational and awareness programmes on cybersecurity threats and cyber hygienic behaviour should be expanded and where possible synchronised across the EU. The most effective way to integrate cybersecurity education in existing educational programmes should be researched beforehand.
- There are currently too few education and training programmes to train the number of professionals necessary. The lack of a transparent and common **classification system** for these programmes further hampers their ability to help close the shortfall.
- Best practices on how to connect those responsible for education with those responsible for cybersecurity, who are often not the same, should be exchanged regularly at the European level.

[3] The Manifesto can be found on the GFCE's website.

It was concluded that there should be a comprehensive approach to **standardisation and certification**, including both technical (product) standards and process standards. The current proliferation of different national standards has led to fragmentation and hinders innovation. EU-wide standards are therefore preferable. The recent communication from the European Commission on ICT standardisation was therefore encouraged. In addition, governments can stimulate more secure products by including cybersecurity demands in their procurement processes.

In addition to the European Commission's efforts to work towards such EU-wide standards, two other points were discussed.

1. A structured approach to ensure software is secure from the designing to implementation phase can contribute to safe hardware and software. Initiatives such as the Secure Software Framework are therefore encouraged, and could also be spread throughout the EU.
2. As not all products serve the same purpose, they might also need different safeguards to ensure their security. While certification would suit certain critical components and systems, a baseline approach would suit other ICT products. For the next steps in the standards and certification field, the Commission is encouraged to include this distinction in its proposals.

Capacity building

Simultaneous to the EU's efforts to enhance its internal cybersecurity strategy, it was recommended the EU and its Member States continue their internal capacity-building on prevention, defence and response. Clear points of contact, also at political and strategic level, are desirable.

Due to cybersecurity being as strong as the weakest link, we should also focus on external capacity-building efforts through initiatives such as the Global Forum on Cyber Expertise (GFCE). These efforts should focus on bringing together the various parties in non-EU countries and on raising the maturity level of CSIRTs. The latter can also be effective when targeted towards EU Member States CSIRTs, which will have additional tasks after the implementation of the NIS Directive.